

Sufficiently Myopic Adversaries are Blind

Bikash Kumar Dey, Sidharth Jaggi, Michael Langberg

Abstract

In this work we consider a communication problem in which a sender, Alice, wishes to communicate with a receiver, Bob, over a channel controlled by an adversarial jammer, James, who is *myopic*. Roughly speaking, for blocklength n , the codeword X^n transmitted by Alice is corrupted by James who must base his adversarial decisions (of which locations of X^n to corrupt and how to corrupt them) not on the codeword X^n but on Z^n , an image of X^n through a noisy memoryless channel. More specifically, our communication model may be described by two channels. A memoryless channel $p(z|x)$ from Alice to James, and an *Arbitrarily Varying Channel* from Alice to Bob, $p(y|x, s)$ governed by a state S^n determined by James. In standard adversarial channels the states S^n may depend on the codeword X^n , but in our setting S^n depends only on James's view Z^n .

The myopic channel captures a broad range of channels and bridges between the standard models of memoryless and adversarial (zero-error) channels. In this work we present upper and lower bounds on the capacity of myopic channels. For a number of special cases of interest we show that our bounds are tight. We extend our results to the setting of *secure* communication in which we require that the transmitted message remain secret from James. For example, we show that if (i) James may flip at most a p fraction of the bits communicated between Alice and Bob, and (ii) James views X^n through a binary symmetric channel with parameter q , then once James is “sufficiently myopic” (in this case, when $q > p$), then the optimal communication rate is that of an adversary who is “blind” (that is, an adversary that does not see X^n at all), which is $1 - H(p)$ for standard communication, and $H(q) - H(p)$ for secure communication. A similar phenomenon exists for our general model of communication.

Keywords: *Arbitrarily Varying Channels, Myopic Jamming, Information Theoretic Secrecy*

I. INTRODUCTION

In the study of point-to-point communication, a sender Alice wishes to transmit a message U to a receiver Bob over a noisy channel governed by a jammer James. To do so, she encodes U into a length- n vector X^n and transmits it over the channel, resulting in the received word Y^n . Two types of channel models that have seen significant attention over the last decades are the memoryless channel model, e.g., [2] in which the channel is governed by a conditional distribution $p(y|x)$ which is completely oblivious [3] (or “blind”) of the message X^n being transmitted and the adversarial (omniscient) channel model in which James is thought of as an adversarial entity who can maliciously design the error imposed to fit the specific codeword transmitted, [4]. While the capacity of the former model is well-understood, that of the latter encompasses numerous open problems in coding and information theory. This state of affairs has lead to the study of several channel models that conceptually lie between the two extreme communication models, those in which the channel is oblivious of the transmitted codeword X^n and those in which the channel acts as an adversarial jammer. These include arbitrarily varying channels (AVCs), e.g. [5]–[8], causal channels, e.g. [9]–[16], and computationally limited channels, e.g. [17].

Inspired by the study of Sarwate [18], in this work we consider the model of *myopic* adversarial jammers. In the myopic setting, the jammer James is still a malicious entity that wishes to carefully design his error to corrupt communication, however his view of the codeword X^n is limited in the sense that it is masked through a noisy memoryless channel $p(z|x)$. If the channel between Alice and James is of full rate, the myopic model reduces to that of the standard omniscient adversarial model, and if it is of zero rate, the myopic model captures the model of a “blind” (or “oblivious”) adversary that has no knowledge whatsoever on the codeword X^n transmitted.

Formally, the myopic model is described by two channels. A memoryless channel $p(z|x)$ from Alice to James, and an AVC from Alice to Bob. The AVC is modeled by a state channel $p(y|x, s)$, where the vector of states S^n (one state for each time step) is determined by James as a function of his masked view Z^n of the transmitted codeword X^n . See Figure 1.

In this work we study the capacity of myopic adversarial channels. We start by studying a natural binary myopic channel in which (i) James may flip at most a p fraction of the bits communicated between Alice and Bob, and (ii) James views X^n through a binary symmetric channel with parameter q (i.e., $BSC(q)$). Namely, in our notation, the Hamming weight of S^n is at most pn , $p(z|x) = q$ for $z \neq x$, and $p(y|x, s) = 1$ iff $y = x + s$ (and otherwise 0). We aim to characterize the capacity of the channel under varying values of q , our limitation on the noise level to James. When $q = 0$, namely when James has full knowledge of the codeword X^n , the channel reduces to the omniscient adversarial channel for which the capacity is a central open problem in coding theory and only upper and lower bounds on capacity exist [19]–[21]. When $q = 1/2$, namely when James is blind, it is shown in [3], [7] that the capacity equals that of the channel in which James flips bits randomly, i.e. the $BSC(p)$, which equals $1 - H(p)$.

The focus of this work is in the study of intermediate values of q . In a nutshell, we present a dichotomous behavior of the channel. If James is “sufficiently myopic” then the optimal communication rate is that of a blind James, namely $1 - H(p)$. Specifically, we show that an optimal rate of $1 - H(p)$ is achievable as long as $q > p$. If on the other hand $q < p$, then the

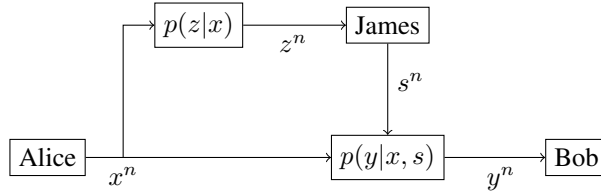


Fig. 1. The myopic channel model

capacity of the myopic channel equals that of the omniscient channel,¹ which is known to be bounded away from $1 - H(p)$ for all p , and in fact equals 0 for all $p > 1/4$. We extend our results to the setting of secure communication in which one requires that the transmitted message remain secret from James. In this extended setting we show a similar phenomena: as long as $q > p$ the capacity equals that obtained for blind adversaries (which is $H(q) - H(p)$).

We then turn to study the myopic model in its full generality, for general memoryless channels $p(z|x)$ connecting Alice and James, and general state channels $p(y|x, s)$ connecting Alice and Bob. For the general setting we obtain upper and lower bounds on capacity, both in the standard setting of communication, and in that of secure communication. As an additional case study, we study the setting in which the channel to James is a binary erasure channel $BEC(q)$, and James can erase up to a fraction p of the transmitted bits observed by Bob. For this special case, through a refinement of our arguments, we show that the capacity is $1 - p$ if $q > p$; and for $q < p$, the deterministic capacity is the same as that for an omniscient adversary. We also consider some more general binary input adversarial channels to study communication rates as well as secrecy rates. In these channels, James can erase as well as flip some fractions of bits. His own observation may be over an arbitrary binary input channel.

As mentioned above, the work most relevant to ours is that of Sarwate [18] in which the myopic channel model is studied under the assumption that Alice and Bob hold shared randomness that is not known to James (i.e., under the assumption of randomized coding). In this setting, a single-letter characterization to the randomized coding capacity is obtained. As with our study, the results in [18] bridge between the randomized capacity when the adversary James is assumed to be blind and that when James has full knowledge of the codeword transmitted.

Although our study was inspired by, and builds on, that of [18], it differs from [18] in two important aspects. Primarily, and most importantly, we study the case of deterministic codes (in which there is no shared randomness between Alice and Bob). The study of deterministic codes introduces many challenges that do not exist in the case of randomized codes, and involves a new set of analytical tools in its analysis. Secondly, we study the general case in which the codewords X^n of Alice and the state space S^n of James are constrained. Our enhanced setting was explicitly left open in [18].

Another model related to our work is the study of the wiretap channel of type II with an active eavesdropper. Aggarwal et al. [22] considers a model with an adversary who can choose a p fraction of bits to observe and also erase these bits. They showed that any rate upto $1 - p - H(2p)$ can be achieved. In our notation, their model has $q = 1 - p$ fraction of erasures in James' channel. If James experiences random erasures, then Theorem III.10 guarantees a secrecy rate upto $(1 - p) - p = 1 - 2p$. However, in [22] James has the additional power of choosing which bits to observe. As a special case of Theorem III.13, we are able to obtain rate $1 - 2p$ on the model of [22] as well (see Remark V.4). Additional works that address the action of myopic adversaries include [23] which considers the study of the wiretap channel of type II with an active eavesdropper that can flip bits. Theorem III.13 generalizes their main result to an active eavesdropper who can erase as well as flip bits. The work in [24], studies a different model of active myopic adversaries in which there are two non-cooperating adversarial entities, the Eavesdropper and the Jammer. In a nice sequence of works by Boche² et al [25]–[27] the problem of secure communication in the presence of a myopic jammer is also considered, but in general in the models considered either common randomness between the transmitter and the receiver is necessary, or only multi-letter capacity characterizations are derived (or both). Also, [28], [29] consider myopicity in the context of AWGN channels. For specific channels over sufficiently large alphabets on which the attacks are either additive (e.g., [30]–[35], summarized in [36]), or “overwrite” (e.g., [37], [38], summarized in [39]), more is known; computationally efficient codes meeting information-theoretic bounds are known. See Table I for a summary of previous related work.

Our paper is structured as follows. In Section II we give a precise model for the myopic setting. In Section III we state our main results (which are also summarized in Table I). Our results are first presented for the special binary symmetric error case discussed above and then in full generality. We also discuss a refinement of the general arguments to an erasure-erasure channel, and other binary input channels with erasing and flipping adversary. Section IV presents the proof of the main result for the binary case. Section V presents the proof of the lower bound for the general model.

¹To be precise, the above dichotomous behavior is proven to hold for deterministic codes. For codes that allow randomness at encoder (which is *not* shared with the receiver), known as stochastic codes, we leave open the question whether one can obtain rates higher than those of the omniscient adversary for the case $q < p$.

²From whom we also borrow the idea of calling the jammer James.

		Channel: Alice to James	Channel: Alice to Bob	Common randomness available?	Eavesdropper and jammer coordinate?	Reliable throughput	Reliable + secure throughput	Comments
Binary input channels	[2] Sha49	–	BSC(p)	–	–	$1 - H(p)$	–	Baseline random noise channels
		–	pn erasures	–	–	$1 - p$	–	
	[19] Gil52, [20] Var57, [21] McERRW77	Perfect channel	pn bit-flips	No	Yes	$\geq 1 - H(2p),$ $\leq LP(2p)$	–	Baseline adversarial noise channels
		Perfect channel	BEC(p)	No	Yes	$\geq 1 - H(p),$ $\leq LP(p)$	–	
	[7] CsiN88 [3] Lan08	No channel	pn bit-flips	No	–	$1 - H(p)$	–	“Oblivious” jammers
	[22] AggLCP09	James can observe and erase any pn bits of his choice		No	Yes	–	$1 - p - H(p)$	Wiretap type II with erasing adversary
Our results: binary input	[23] Wan16	James chooses $p_r n$ bits to see	$p_w n$ bit flips	No	Yes	–	$1 - p_r - H(p_w)$	Wiretap type II with flipping adversary
	$C(q, p), q > p$	BSC(q)	pn bit flips	No	Yes	$1 - H(p)$	$H(q) - H(p)$	Th. III.1, III.3
	$CE(q, p), q > p$	BEC(q)	pn erasures	No	Yes	$1 - p$	$q - p$	Th. III.8, III.10
	CEF ($p_{Z X}, p_e, p_w$)	$p_{Z X}$	$p_e n$ erasures & p_w flips	No	Yes	$(1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right)\right)^\dagger$	$H(X Z) - p_e$ $+ p_e H\left(\frac{p_w}{1 - p_e}\right)$ $- H\left(\frac{p_w}{1 - p_e}\right)$	Th. III.11, III.12
Other channels (large alphabets)		James can choose $p_r n$ symbols to see	$p_e n$ erasures, $p_w n$ flips	No	Yes	–	$1 - p_r - p_e$ $+ p_e H\left(\frac{p_w}{1 - p_e}\right)$ $- H\left(\frac{p_w}{1 - p_e}\right)$	Wiretap type II with erasing and flipping adv. Th. III.13
	[30], [36]	James can choose $p_r n$ symbols to see	Additive noise over \mathbb{F}_q , $p_w n$ symbol errors	No	Yes	$1 - p_w$	$1 - p_r - p_w$	q “sufficiently large”, Computationally efficient
General Discrete Memoryless Channels	[37]–[39]	James can observe $n(p_{ro} + p_{rw})$ symbols of his choice	Additive and overwrite noise over \mathbb{F}_q , $n(p_{wo} + p_{rw})$ symbol errors	No	Yes	$f_1(p_{ro}, p_{rw}, p_{wo})$	$f_2(p_{ro}, p_{rw}, p_{wo})$	q “sufficiently large”, Computationally efficient, $f_1(\cdot), f_2(\cdot)$ – complete characterization
	[7] CsiN88	No channel	General $p_{Y X,S}$	No	–	$\max_{p(x)} \min_{p(s)} I(X; Y)$	–	Max/min over permissible input/state constraints resp.
General Discrete Memoryless Channels	[24] MolBL09, [40] LiaKPS09	$p_{Z X,S}$	$p_{Y X,S}$	Yes	No	–	$\geq \max_{p(x,u)} (\min_s I(U; Y) - \max_s I(U; Z))$ $\leq \max_{p_X} \min_{p_S} I(X; Y Z)$	$\forall s, U \leftrightarrow X \leftrightarrow (Y, Z),$ “Degraded” wiretapper
	[18] Sar10	$p_{Z X}$	$p_{Y X,S}$	Yes	Yes	$\max_{p_X} \min_{p_{S Z}} I(X; Y)$	–	
	$C(p_{Z X}, \mathcal{W})$ (our result)	$p_{Z X}$	state constraint: \mathcal{W}	No	Yes	$\max_{p_x} \min_{p_{S Z}} I(X; Y)^\ddagger$	$\max_{p_x} \min_{p_{S Z}} (I(X; Y) - I(X; Z))^*$	Th. III.4, III.6

TABLE I

SUMMARY OF MODELS AND RESULTS. (\dagger) UNDER THE CONDITION $1 - H(X|Z) < (1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right)\right)$; (\ddagger) UNDER THE CONDITIONS: $\forall p_{S|Z} \in \mathcal{W}_{S|Z} : I(X; Z) < I(X; Y)$, AND $\max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y, S) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) < H(X|Z)$; (*) UNDER THE CONDITION $\max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y, S) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) < H(X|Z)$.

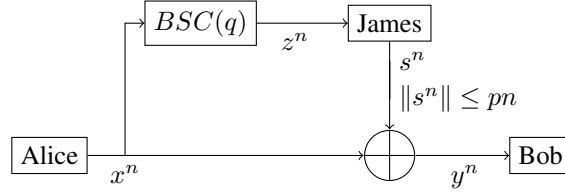


Fig. 2. The binary symmetric error channel $C(q, p)$

II. MODEL

The myopic channel is defined by its input alphabet \mathcal{X} , output alphabet to James \mathcal{Z} , state alphabet \mathcal{S} , output alphabet to Bob \mathcal{Y} , probability distribution for the channel connecting Alice and James $p(z|x)$, probability distribution $p(y|x, s)$ for the channel connecting Alice and Bob, the state constraint \mathcal{W} , and the input constraint \mathcal{V} . The three parties of the channel, Alice, Bob, and James are described below (see Figure 1).

Alice's encoder: Alice has a message U uniformly distributed in $\{0, 1\}^{nR}$ that she wants to transmit to Bob; R denotes the rate of her message, and n the block-length of Alice's transmissions. To effect this communication, Alice encodes her message using an encoder $Enc : \{0, 1\}^{nR} \rightarrow \mathcal{X}^n$ to output a transmitted vector $X^n = Enc(u)$. We emphasize that Alice's encoder is deterministic. The encoder has to satisfy the constraint $\text{type}(X^n) \in \mathcal{V}$, where \mathcal{V} is a set of types over the alphabet \mathcal{X} .

Channel from Alice to James: James observes the output of X^n passing through a memoryless channel $p(z|x)$. More precisely, the channel law is given as $Pr(Z^n|X^n) = \prod_t p(z_t|x_t)$. Based on James's non-causal observation Z^n , he chooses a length- n state vector S^n . The state vector S^n is restricted to have $\text{type}(S^n) \in \mathcal{W}$, where \mathcal{W} is a set of types over the alphabet \mathcal{S} .

Channel from Alice to Bob: Bob observes the output Y^n obtained through the channel $p(y|x, s)$. More precisely, for state $S^n = (s_1, \dots, s_n)$ the channel law is given as $Pr(Y^n|X^n, S^n) = \prod_t p(y_t|x_t, s_t)$.

Successful communication: Given Y^n , Bob decodes a message $\hat{u} \in \{0, 1\}^{nR}$. Communication is considered successful if the transmitted message u equals \hat{u} . The average error in communication is defined as $\varepsilon = \frac{1}{2^{nR}} \sum_u Pr(u \neq \hat{u})$.³ Rate R is achievable over the myopic channel if for any $\varepsilon > 0$ there exists a block length n such that the average error in communication is at most ε . The channel capacity is the supremum of all achievable rates.

Secrecy: At times we will study the secrecy (i.e., secure) capacity between Alice and Bob. In this setting, in addition to correct decoding, we require that James's view Z^n be almost independent of Alice's message u , namely that $\frac{1}{n} I(Z^n; U) < \varepsilon$.

III. OUR RESULTS

In what follows we present our results. The results are presented first for the special binary symmetric error myopic channel (Sec. III-A) discussed in the Introduction, and then in generality (Sec. III-B). We also present refinements of our general results for a binary erasure-erasure model, and more general binary AVC where James can erase and flip some fractions of transmitted bits in Subsection III-C and Subsection III-D respectively.⁴

A. The myopic binary $C(q, p)$ channel

Our studies begin with the binary channel $C(q, p)$ (Fig. 2) characterized by the pair of parameters (q, p) in which (i) James views X^n through a binary symmetric channel with parameter q (i.e., $BSC(q)$), and (ii) James may flip at most a fraction p of the bits communicated between Alice and Bob. Namely, in our notation, we set $\mathcal{X} = \mathcal{Z} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $p(z|x) = q$ for $z \neq x$, $p(y|x, s) = 1$ iff $y = x + s$ (and otherwise 0), and $\mathcal{W} = \{(1 - p', p') | p' \leq p\}$ (i.e., $\text{type}(S^n) \in \mathcal{W}$ if and only if $\|S^n\| \leq pn$) where $\|\cdot\|$ denotes the Hamming weight).

We first study the case $q > p$:

Theorem III.1. *For $q > p$, the capacity of the binary myopic adversarial channel $C(q, p)$ is $1 - H(p)$. The capacity is achieved by random codes with input distribution $Ber(1/2)$.*

To prove Theorem III.1 we must present both an upper and a lower bound on capacity. The upper bound is relatively simple and follows from the fact that James may roughly mimic a memoryless $BSC(p)$ (no matter what q is). Specifically, James can completely neglect his view Z^n and just construct a state vector uniformly at random among those with type $(1 - p, p)$.

³Notice that in the setting of deterministic code design the average error criteria is essential for the study of the myopic model (in which we assume that James bases his decisions on a corrupted view of X^n), as otherwise, in the study of maximum error, James may neglect Z^n and focus his strategy on a single transmitted codeword, yielding the channel $p(z|x)$ irrelevant to the study of capacity. This state of affairs does not hold once stochastic coding is considered. Connections exist between the study of deterministic codes under the average error criteria and stochastic codes under the maximum error criteria in the context of AVCs, e.g., [6]. In this work we focus on deterministic codes (which we prove are optimal for several of the settings we study).

⁴All our results on bit-flip and/or erasure channels can be generalized to q -ary additive and erasure channels, i.e., where James can erase some fraction of symbols and/or add arbitrary symbols of his choice to some fraction of symbols. In the interest of brevity we do not present these straightforward generalizations.

The converse of the channel coding theorem now shows that the rate in this case is bounded above by $1 - H(p)$. Our main contribution in the study of $C(q, p)$ is in the achievability part of Theorem III.1 in which we show that one can obtain rates arbitrarily close to $1 - H(p)$. The technical proof as well as a proof outline are given in Section IV.

We next study the case of $q < p$. Here, we show that the capacity equals that of the omniscient adversary.

Theorem III.2. *For $q < p$, the deterministic coding capacity of the binary myopic adversarial channel $C(q, p)$ is the same as that of the binary adversarial channel with an omniscient adversary.*

Proof: We assume successful communication at rate R over $C(q, p)$ and show that R is achievable in the omniscient channel model as well. Consider the code that allows communication at rate R . The same code must also allow communication at rate R over $BSC(q)$ (this follows from the fact that $q < p$ and thus James can roughly mimic $BSC(q)$, just as described above in the converse to Theorem III.1). Since for such an adversarial action, Bob can still decode X^n , this implies that James, who views X^n through a $BSC(q)$ is able to decode X^n as well, implying, in turn, that James is actually omniscient. ■

We finally turn to study the context of secure communication. Here, we first consider the binary symmetric broadcast channel with independent BSC to Bob and James with cross-over probabilities p and q respectively. Then it is well known [41] that the message transmission capacity to Bob under the secrecy condition is $H(q) - H(p)$. An achievability scheme in this case is to append the nR bits of message with $n(1 - H(q))$ bits of private randomness and encode the resulting string with a random channel code of rate $1 - H(p)$.

In our channel $C(q, p)$, for $q > p$, the secrecy capacity is also $H(q) - H(p)$. The encoding can be done in the same way as before: appending random bits to the message and then encoding using a random code. James can not learn anything about the message by the secrecy results in the random channel case discussed above. Since James is sufficiently myopic, by Theorem III.1, Bob can decode the message and the private randomness irrespective of James's strategy. So, we have

Theorem III.3. *For $q > p$, the binary myopic channel $C(q, p)$ has secrecy capacity $H(q) - H(p)$.*

B. General myopic channels

We now turn to present our results for the myopic model in full generality. We consider the setup where James's channel is given by $p_{Z|X}$, and his state S^n is constrained to have a type in the set \mathcal{W} . We denote this channel by $C(p_{Z|X}, \mathcal{W})$. To obtain single letter upper and lower bounds on the capacity of myopic channels we consider the types of the vectors X^n , Z^n , S^n , and Y^n , and certain distributions on them. Our achievability scheme uses a random code governed by the single letter distribution $p_X \in \mathcal{V}$. Let $p_{Z|X}$ be James's channel law (we now explicitly specify the channel as a subscript to avoid confusion). The distributions, p_X and $p_{Z|X}$ give rise to a joint distribution p_{XZ} and a marginal distribution p_Z . Recall that \mathcal{W} is the set of state types of S^n which James may impose. Let $\mathcal{W}_{S|Z}$ be the set of conditional distributions $p_{S|Z}$ which results in a marginal distribution p_S in the set \mathcal{W} . Namely, $p_{S|Z}$ is in $\mathcal{W}_{S|Z}$ if and only if

$$p_S(\cdot) = \sum_{x,z} p_X(x)p_{Z|X}(z|x)p_{S|Z}(\cdot|z) \in \mathcal{W}$$

Finally, we use $p_{Y|XS}(y|x, s)$ which is given as part of the channel definition. Note that p_X and $p_{S|Z}$ define a joint single letter distribution over random variables X, Z, S, Y defined by $p_X p_{Z|X} p_{S|Z} p_{Y|XS}$.

We are now ready to present our results for the general model. Our first theorem addresses achievability. For technical reasons, we focus only on "state-deterministic channels", i.e. where Y^n is a deterministic function of (X^n, S^n) . We elaborate on channels which are not state-deterministic in Section V.

Theorem III.4. *For state-deterministic $p_{Y|XS}$ a rate R is achievable if there exists a $p_X \in \mathcal{V}$ such that*

$$\begin{aligned} (a) \quad & \forall p_{S|Z} \in \mathcal{W}_{S|Z} : R < I(X; Y). \\ (b) \quad & \forall p_{S|Z} \in \mathcal{W}_{S|Z} : I(X; Z) < I(X; Y). \\ (c) \quad & \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y, S) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) < H(X|Z). \end{aligned}$$

Such a rate is achievable using random codes generated using the input distribution p_X .

Our proof of Theorem III.4 is along similar lines as that of Theorem III.1, and is presented in Sec. V. The theorem guarantees the maximum rate $I(X; Y)$ (condition (a)) against an oblivious adversary with state constraint, provided the state constraint satisfies the two myopicity conditions (b) and (c). Here condition (b) says that James's channel should be worse than Bob's channel, i.e., James's view should be less 'informative' than Bob's. This corresponds to the condition $q > p$ in the binary case in Theorem III.1. Though condition (c) also says something similar in nature, its exact form is not intuitive. It comes due to a technical requirement in the proof (see Remark V.4).

We now give an upper bound obtained by considering only memoryless feasible jamming strategies. The proof is obvious, and is omitted.

Theorem III.5. A rate R is achievable only if there exists a $p_X \in \mathcal{V}$ such that $\forall p_{S|Z} \in \mathcal{W}_{S|Z} : R < I(X; Y)$.

Using a similar argument as in the binary case (Theorem III.3), we obtain the following achievability result for secrecy rates.

Theorem III.6. For state-deterministic $p_{Y|XS}$ a secrecy rate R is achievable if there exists a $p_X \in \mathcal{V}$ such that

$$(a) \forall p_{S|Z} \in \mathcal{W}_{S|Z} : R < I(X; Y) - I(X; Z). \\ (b) \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y, S) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) < H(X|Z).$$

Remark III.7. The proof of secrecy for rates under $I(X; Y) - I(X; Z)$ is following similar encoding and arguments as that for wiretap channels. For wiretap channels, it is known that this can be improved to the maximum of $I(U; Y) - I(U; Z)$ over all $p(u)p(x|u)$. However, our proof (of Theorem III.6) uses a state-deterministic $p_{Y|XS}$. Introducing an auxiliary random variable U will result in an effective probabilistic AVC $p_{Y|US}$, for which our present proof does not hold. Please also see footnote 5.

C. Binary erasure-erasure channels

Communicating securely in the presence of an active eavesdropper has attracted some attention in the recent literature (e.g. [22], [23]). Hence in this and the next subsection we remark on the implications of our techniques/results for some binary-input channels. One of the challenges is that unlike in the binary symmetric case (Theorem III.1), for general myopic channels, our lower bound (Theorem III.4) does not meet the upper bound (Theorem III.5). This is due to the difficulty of finding a single-letter expression for a counting argument in the proof of Lemma V.2.

For an erasure-erasure channel (referred to as $CE(q, p)$) where James's channel is a $BEC(q)$, and he can erase at most a p fraction of the transmitted bits, Theorem III.4 guarantees rates upto $1 - p$ only if $q > p + H(p)$, whereas the upper bound of $1 - p$ in Theorem III.5 is valid whenever $q > p$. This gap can be eliminated by careful analysis using specific properties of erasure channels. As a result, we have the capacity results as given below.

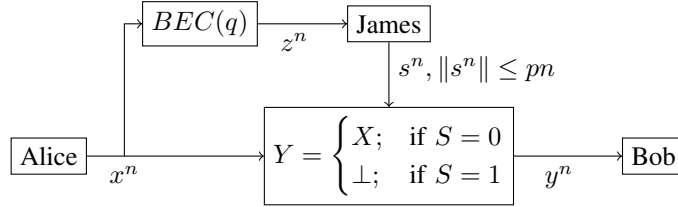


Fig. 3. The binary erasure-erasure adversarial channel $CE(q, p)$

Theorem III.8. For $q > p$, the capacity of the binary erasure-erasure channel $CE(q, p)$ is $1 - p$. The capacity is achieved by random codes with input distribution $Ber(1/2)$.

The proof of this result follows as a special case of (Theorem III.4) with a specific refinement in Lemma V.2 as discussed in Remark V.4.

The next two theorems follow using similar arguments as those of Theorem III.2 and Theorem III.3 respectively. The proofs are thus omitted.

Theorem III.9. For $q < p$, the deterministic coding capacity of the binary erasure-erasure adversarial channel $CE(q, p)$ is the same as that of the binary erasing adversarial channel with an omniscient adversary.

Theorem III.10. For $q > p$, the binary erasure-erasure myopic channel $CE(q, p)$ has secrecy capacity $q - p$.

D. More general binary input channels

Similar to the binary erasure-erasure channel $CE(q, p)$, we may improve on Theorems III.4, III.6 for other channels as well. A number of examples are given below.

1) *Erasing and flipping adversary*, $CEF(p_{Z|X}, p_e, p_w)$: Let us consider a binary input setup $CEF(p_{Z|X}, p_e, p_w)$ where James's channel is given by $p_{Z|X}$, and James can erase upto a fraction p_e and flip upto a fraction p_w of the transmitted bits ($p_e + p_w \leq 1$). The corresponding random channel (binary symmetric error and erasure channel) has a capacity $(1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right) \right)$.

Theorem III.11. For $CEF(p_{Z|X}, p_e, p_w)$, if

$$1 - H(X|Z) < (1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right) \right)$$

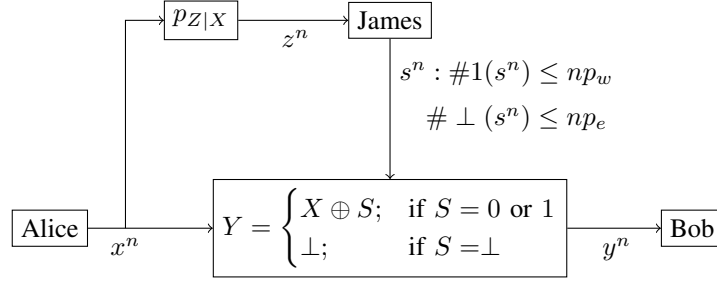


Fig. 4. The binary input channel with erasing and flipping adversary, $CEF(p_{Z|X}, p_e, p_w)$

then the capacity is $(1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right)\right)$.

The proof is similar to the general myopic results, and the key element in the proof is outlined in Remark V.4.

2) *Secrecy capacity for erasing and flipping adversary, $CEF(p_{Z|X}, p_e, p_w)$* : We now consider the secrecy capacity of $CEF(p_{Z|X}, p_e, p_w)$, i.e., when James's channel is $p_{Z|X}$, and the James can erase upto a fraction p_e and flip upto a fraction p_w of the transmitted bits. Using a randomly constructed code to encode the message and private randomness we obtain (see Remark V.4 for details).

Theorem III.12. *For the channel $CEF(p_{Z|X}, p_e, p_w)$, the secrecy rate $H(X|Z) + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right)$ is achievable. In particular, for the channel $CEF(BEC(q), p_e, p_w)$, the secrecy rate $q + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right)$ is achievable.*

3) *Wiretap channel of type II with erasing and flipping adversary, $WCEF-II(p_r, p_e, p_w)$* : We denote the wiretap channel of type II with active adversary who can erase and flip bits as $WCEF-II(p_r, p_e, p_w)$. Here instead of James's channel being a random erasure channel, James can also choose a $p_r = 1 - q$ fraction of the transmitted bits to view/read, and he can erase upto a fraction p_e and flip upto a fraction p_w of the transmitted bits. This is a generalization of the models studied in [22], [23] for Wiretap channel of type II with active adversaries.

Theorem III.13 (Wiretap channel of type II with erasing and flipping adversary). *For $WCEF-II(p_r, p_e, p_w)$, the rate $1 - p_r + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right)$ is achievable.*

This result is of independent interest as it generalizes results on the wiretap channel of type II with active adversary [22], [23]. Our general proof technique together with the argument in Remark V.4 implies this result. As a special case, in the model $WCEF-II(p, p, 0)$, James can observe upto a p fraction of bits of *his choice* and he can also erase a p fraction of bits. For a more restricted James (who has to erase the same bits that he observes), Aggarwal et al. [22] showed that rates upto $1 - p - H(p)$ can be achieved. Theorem III.13 improves this to $1 - 2p$. As another special case, in the model $WCEF-II(p_r, 0, p_w)$, Theorem III.13 gives an achievable rate of $1 - p_r - H(p_w)$, which is same as the achievable rate in [23].

IV. PROOF OF THEOREM III.1

The converse follows using the converse for BSC_p (as discussed in Section III). We first present a sketch of the achievability in Subsection IV-A, and then in Subsection IV-B we give a formal proof. Our proof is summarized in Figure 6.

A. Proof sketch for Theorem III.1

We now sketch the proof for the achievability of rates arbitrarily close to $1 - H(p)$ over $C(q, p)$ when $q > p$ (Theorem III.1). For a precise proof, and also for the precise definition of some of the ideas, we refer the reader to the technical proof appearing in Subsection IV-B.

Our code construction uses a uniformly chosen codebook over $\{0, 1\}^n$ and our decoder associates with each received word Y^n its closest codeword X^n . We now show that with high probability over code design, such codes are sufficient for communication at any rate $R = 1 - H(p) - \epsilon$ and average error ϵ where $\epsilon > 0$ is arbitrarily small. In what follows, many of the statements we make occur with high probability over code design (and not necessarily with probability 1) even though at times we do not state so explicitly.

Consider a codeword X^n transmitted by Alice. This codeword passes through the channel to James, and James receives the corrupted version Z^n of X^n . The fact that $q > p$ (or more precisely that $1 - H(q) < 1 - H(p)$) now implies that there are approximately $2^{n(H(q) - H(p))}$ codewords that are *consistent* with James's view Z^n (Lemma IV.2). Namely, that there are an exponential number of codewords X^n , that from James's perspective, may have been transmitted by Alice that would have

and those that were confusing them (denoted by \hat{X}^n). To overcome this difficulty, we partition the set \mathcal{M}_{og} into disjoint sets and study the effect of one set in the partition on another. Then by a combination of similar list decoding arguments and additional counting arguments, we can show that only an exponentially small fraction of codewords $X^n \in \mathcal{M}_{og}$ are confused by a codeword $\hat{X}^n \in \mathcal{C}$. The claimed list decoding properties above hold with extremely high probability of $1 - 2^{-\beta n^2}$ on code design. This allows us to use the union bound on several assumptions made throughout the discussion (e.g., the values of d , z^n and s^n).

B. Achievability proof of Theorem III.1

We now prove that any rate $R < 1 - H(p)$ can be achieved. Without loss of generality, we assume that $R = 1 - H(p) - \epsilon > 1 - H(q)$. We also assume, without loss of generality, that ϵ is sufficiently small.

Code construction: The code consists of 2^{nR} vectors $X^n(w); w = 1, 2, \dots, 2^{nR}$, all selected independently with i.i.d. $\sim \text{Bernoulli}(1/2)$ components.

Encoding: Alice encodes message W with $X^n(W)$ and transmits.

Decoding: Let the vector received by Bob be Y^n . If Bob finds a unique \hat{W} such that $X^n(\hat{W})$ is within distance $(p + \epsilon_1)n$ from Y^n , then he declares \hat{W} as the decoded message. Otherwise he declares error. Here ϵ_1 is a predetermined constant (that is set to be sufficiently small).

For any subset of messages $M \subseteq \{1, 2, \dots, 2^{nR}\}$, we define its codewords as

$$X^n(M) := \{X^n(w) | w \in M\}.$$

After observing Z^n , James can find all the codewords which are jointly typical with it. With high probability, the transmitted codeword belongs to that set. We define, for any z^n, d , the ball and the shell

$$\begin{aligned} \mathcal{B}(z^n, d) &:= \{x^n \in \{0, 1\}^n : d_H(x^n, z^n) \leq d\}, \\ \mathcal{Sh}(z^n, d) &:= \{x^n \in \{0, 1\}^n : d_H(x^n, z^n) = d\}. \end{aligned}$$

Let D denote the random variable $d_H(X^n(W), Z^n)$. Let ϵ_2 be a sufficiently small constant. We define the following events

$$\begin{aligned} \mathcal{E}_{C1}(z^n, d) &:= \left\{ 2^{n(H(d/n) + R - 1 + \epsilon_2)} \geq |\{w : X^n(w) \in \mathcal{Sh}(z^n, d)\}| \geq 2^{n(H(d/n) + R - 1 - \epsilon_2)} \right\} \\ \mathcal{E}_{C1} &:= \cap_{z^n, d: |d - qn| \leq \epsilon_1 n} \mathcal{E}_{C1}(z^n, d) \\ \mathcal{E}_D &:= \{(q - \epsilon_1)n \leq D \leq (q + \epsilon_1)n\}, \end{aligned}$$

$\mathcal{Sh}(Z^n, D)$ is the spherical shell around James's received vector where the transmitted codeword lies. The code satisfies \mathcal{E}_{C1} with high probability according to Lemma IV.2 below. We assume that an oracle reveals to James some additional information, and prove our achievability under this stronger adversary. For every possible z^n , and d satisfying $(q - \epsilon_1)n \leq d \leq (q + \epsilon_1)n$, the oracle partitions the set of messages

$$M_s(z^n, d) = \{w : X^n(w) \in \mathcal{Sh}(z^n, d)\}$$

with codewords on the shell $\mathcal{Sh}(z^n, d)$ into disjoint subsets $M_{og}^{(1)}(z^n, d), M_{og}^{(2)}(z^n, d), \dots, M_{og}^{(\lambda(z^n, d))}(z^n, d)$ of size $2^{n\delta}$, except possibly the last subset with smaller size. Here δ is chosen to be small enough to satisfy some requirements to be mentioned later. This partitioning is done deterministically by taking the messages in order of their value, that is, satisfying $w < w'$ for each $w \in M_{og}^{(i)}(z^n, d), w' \in M_{og}^{(i+1)}(z^n, d)$.

Additional information to James from the oracle: The oracle reveals D and the particular subset $\mathcal{M}_{og} = M_{og}^{(i)}(Z^n, D)$ of $M_s(Z^n, D)$ that contains the encoded message W .

We denote the sets

$$\begin{aligned} \mathcal{M}_s &:= M_s(Z^n, D) \\ \mathcal{M}_o &:= \mathcal{M}_s \setminus \mathcal{M}_{og} \end{aligned}$$

We make a few observations prior to our analysis.

O.1 James's view (oracle aided) consists of Z^n received over his channel, and \mathcal{M}_{og}, D received from the oracle.

O.2 Given James's view, the encoded message W is uniformly distributed in \mathcal{M}_{og} .

O.3 Over the random code construction, given the values of $D, Z^n, \mathcal{M}_{og}, \mathcal{M}_s, \mathcal{M}_o$, the codewords $\{X^n(w) | w \in \mathcal{M}_{og}\}, \{X^n(w) | w \in \mathcal{M}_o\}$, and $\{X^n(w) | w \in \mathcal{M}_s^c\}$ are independently and uniformly distributed in respectively $\mathcal{Sh}(Z^n, D), \mathcal{Sh}(Z^n, D)^c$, and $\mathcal{Sh}(Z^n, D)^c$.

First we give three standard lemmas showing that w.h.p., D has a typical value (Lemma IV.1), the spherical shell around Z^n has a typical number of codewords (Lemma IV.2), and that among the partitions of these codewords, the transmitted message is not in the last one - with a smaller size than $2^{n\delta}$ (Lemma IV.3).

Lemma IV.1. *There exists $h_1(\epsilon_1)$ with $h_1(\epsilon_1) \rightarrow 0$ as $\epsilon_1 \rightarrow 0$ s.t. $Pr(\mathcal{E}_D) \geq 1 - 2^{-nh_1(\epsilon_1)}$ for large enough n .*

Proof: The proof follows from standard typicality arguments. ■

Lemma IV.2. *There exists $h_2(\epsilon_1, \epsilon_2)$ s.t. $Pr(\mathcal{E}_{C1}) \geq 1 - 2^{-2^{nh_2(\epsilon_1, \epsilon_2)}}$, where $h_2(\epsilon_1, \epsilon_2) \rightarrow H(q) - H(p)$ as $\epsilon_2, \epsilon_1 \rightarrow 0$.*

Proof: Note that there are at most $n + 1$ possible values of d satisfying the condition in \mathcal{E}_{C1} . Further, there are 2^n possible values of z^n . Let us fix a pair z^n, d . For large enough n , clearly, $2^{n(H(d/n)+R-1+\epsilon_2/2)} \geq E|\{w : X^n(w) \in Sh(z^n, d)\}| \geq 2^{n(H(d/n)+R-1-\epsilon_2/2)}$. Thus by Chernoff bound and by taking the union bound over z^n, d , we have $Pr(\mathcal{E}_{C1}^c) \leq 2^{-(1/6)2^{n(H(q-\epsilon_1)+R-1-\epsilon_2)}} \leq 2^{-2^{nh_2(\epsilon_1, \epsilon_2)}}$ for a suitable $h_2(\epsilon_1, \epsilon_2)$. ■

Given $\mathcal{E}_{C1}, \mathcal{E}_D$, the messages in \mathcal{M}_s are partitioned into exponentially many subsets. Only at most one of those subsets is of smaller size than $2^{n\delta}$. Let us define the event

$$\mathcal{E}_O := \{\mathcal{M}_{og} \neq M_{og}^{(\lambda(Z^n, D))}(Z^n, D)\}$$

that the oracle given set to James is not the last subset (which has possibly smaller size than $2^{n\delta}$) in the partition of $M_s(z^n, d)$. Since given $\mathcal{E}_{C1}, \mathcal{E}_D, \mathcal{M}_s$, the encoded message W is uniformly distributed in \mathcal{M}_s , we have

Lemma IV.3.

$$Pr(\mathcal{E}_O | \mathcal{E}_{C1}, \mathcal{E}_D) > 1 - 2^{-nh_3(\epsilon_1, \epsilon_2)}$$

where $h_3(\epsilon_1, \epsilon_2) = H(q - \epsilon_1) + R - 1 - \epsilon_2 - \delta$.

Let us fix z^n, s^n and d satisfying $|d - qn| \leq n\epsilon_1$. Let us now define an event $\mathcal{E}_{C2}(z^n, d, s^n)$ over the code construction that every subset of size $2^{n\delta}$ in the ordered partition of $M_s(z^n, d)$ has at most only $2^{n(3\delta/4)}$ messages which will undergo decoding error for the respective realizations of D, Z^n, S^n, W . We also define

$$\mathcal{E}_{C2} = \cap_{z^n, d, s^n} \mathcal{E}_{C2}(z^n, d, s^n),$$

where the intersection is over all d satisfying $|d - qn| \leq n\epsilon_1$, all feasible s^n , and all z^n .

We will show in the subsequent analysis that the random code construction guarantees

$$Pr(\mathcal{E}_{C2}^c \cup \mathcal{E}_{C1}^c) \leq 2^{-cn^2} \quad (1)$$

for a positive constant c . Hence, with very high probability over the code construction, the code satisfies the good event $\mathcal{E}_{C1} \cap \mathcal{E}_{C2}$. We will study such codes satisfying $\mathcal{E}_{C1}, \mathcal{E}_{C2}$. For such a code, the probability of error is bounded as

$$\begin{aligned} Pr(Error | \mathcal{E}_{C1}, \mathcal{E}_{C2}) &\leq Pr(\mathcal{E}_D^c | \mathcal{E}_{C1}, \mathcal{E}_{C2}) + Pr(\mathcal{E}_O^c | \mathcal{E}_{C1}, \mathcal{E}_D, \mathcal{E}_{C2}) \\ &\quad + Pr(Error | \mathcal{E}_{C1}, \mathcal{E}_D, \mathcal{E}_O, \mathcal{E}_{C2}) \\ &\leq 2^{-nh_1(\epsilon_1)} + 2^{-nh_3(\epsilon_1, \epsilon_2)} + 2^{-n\delta/4} \end{aligned} \quad (2)$$

Here the first term follows from Lemma IV.1 by noting that \mathcal{E}_D depends on the noise realization in James's channel, and so it does not depend on the code events $\mathcal{E}_{C1}, \mathcal{E}_{C2}$. The second term follows from Lemma IV.3 as the same result holds even when conditioned on \mathcal{E}_{C2} (Conditioned on $\mathcal{E}_{C1}, \mathcal{E}_D$, it is independent of \mathcal{E}_{C2} .) This is because, \mathcal{E}_O depends on the oracle's random choice, and its probability does not change even if the code satisfies the additional property \mathcal{E}_{C2} . Finally, the third term follows from the definition of \mathcal{E}_{C2} .

Hence once (1) is proved, it will imply that with high probability, the randomly generated code will have exponentially small probability of error as guaranteed by (2). This will complete the proof of Theorem III.1.

We now proceed to prove (1). Now,

$$Pr(\mathcal{E}_{C1}^c \cup \mathcal{E}_{C2}^c) = Pr(\mathcal{E}_{C1}^c) + Pr(\mathcal{E}_{C1} \cap \mathcal{E}_{C2}^c)$$

The first term is small by Lemma IV.2. Now, the second term is

$$\begin{aligned}
Pr(\mathcal{E}_{C1} \cap \mathcal{E}_{C2}^c) &= Pr(\cup_{z^n, d, s^n} (\mathcal{E}_{C1} \cap \mathcal{E}_{C2}^c(z^n, d, s^n))) \\
&\leq \sum_{z^n, d, s^n} Pr(\mathcal{E}_{C1} \cap \mathcal{E}_{C2}^c(z^n, d, s^n)) \\
&\leq \sum_{z^n, d, s^n} Pr(\mathcal{E}_{C1}(z^n, d) \cap \mathcal{E}_{C2}^c(z^n, d, s^n)) \\
&= \sum_{z^n, d, s^n} Pr(\mathcal{E}_{C1}(z^n, d)) Pr(\mathcal{E}_{C2}^c(z^n, d, s^n) | \mathcal{E}_{C1}(z^n, d)) \\
&\leq \sum_{z^n, d, s^n} Pr(\mathcal{E}_{C2}^c(z^n, d, s^n) | \mathcal{E}_{C1}(z^n, d)) \\
&= \sum_{z^n, d, s^n} \sum_M Pr(M_s(z^n, d) = M | \mathcal{E}_{C1}(z^n, d)) Pr(\mathcal{E}_{C2}^c(z^n, d, s^n) | \mathcal{E}_{C1}(z^n, d), M_s(z^n, d) = M) \\
&= \sum_{z^n, d, s^n} \sum_M Pr(M_s(z^n, d) = M | \mathcal{E}_{C1}(z^n, d)) Pr(\mathcal{E}_{C2}^c(z^n, d, s^n) | M_s(z^n, d) = M)
\end{aligned}$$

where all the above summations are over d satisfying $|d - qn| \leq n\epsilon_1$, and over M satisfying $2^{n(H(d/n)+R-1+\epsilon_2)} \geq |M| \geq 2^{n(H(d/n)+R-1-\epsilon_2)}$. In the last line, we have used the fact that $M_s(z^n, d) = M$ implies $\mathcal{E}_{C1}(z^n, d)$. Thus to show (1), it is sufficient to show that for some $\beta > 0$, for every such M ,

$$Pr(\mathcal{E}_{C2}^c(z^n, d, s^n) | M_s(z^n, d) = M) \leq e^{-\beta n^2}. \quad (3)$$

We note that for a given M , the partitioning is in increasing order of the message value, and is thus deterministic. There are only exponentially many subsets in its ordered partition as used by the oracle.

We now proceed to prove (3). The messages in M which contribute to $\mathcal{E}_{C2}^c(z^n, d, s^n)$ are classified into two categories. Lemma IV.6 bounds the number of codewords which are decoded wrongly due to confusion with another codeword *outside the same partition* (revealed by the oracle). These codewords include those in the shell (but in another partition) as well as those outside the shell. Lemma IV.7 bounds the number of codewords which are decoded wrongly due to confusion with another codeword *in the same partition* that is revealed by the oracle.

First, we give a basic list-decoding result that will be used in Lemmas IV.6 and IV.7.

Lemma IV.4. *Let A be a set with $2^{\alpha n}$ elements for some $\alpha > 0$, c be a sufficiently large constant, $\nu > 0$, and let X_1, X_2, \dots, X_N be chosen uniformly at random from A where $N = 2^{nR}$. If $V \subset A$ with $|V| \leq 2^{n(\alpha-R-\nu)}$, then $Pr\{|\{i : X_i \in V\}| > cn^2\} \leq e^{-cn^2/6}$.*

The proof follows using the same argument as [3, Lemma A.3].

Corollary IV.5. *With probability at least $1 - 2^{-\beta n^2}$, the code satisfies the property that in every Hamming sphere of radius $(p + \epsilon_1)n$, there are at most cn^2 codewords.*

Lemma IV.6. *There exists $\beta > 0$ such that, for every z^n, d satisfying $|d - qn| \leq n\epsilon_1$, error s^n introduced by James, for every subset M of messages with $2^{n(H(d/n)+R-1+\epsilon_2)} \geq |M| \geq 2^{n(H(d/n)+R-1-\epsilon_2)}$, conditioned on $M_s(z^n, d) = M$, with probability at least $1 - e^{-\beta n^2}$ over the code, for every $i < \lambda(z^n, d)$, there are at most $c^2 n^4$ codewords $X^n(w)$ in $M_{og}^{(i)}(z^n, d)$ for which there is a different codeword $X^n \in M_s^c(z^n, d) \cup (M_s(z^n, d) \setminus M_{og}^{(i)}(z^n, d))$ with*

$$d_H(X^n(w) + s^n, X^n) \leq (p + \epsilon_1)n. \quad (4)$$

Proof: We first prove the statement for codewords in $M_s^c(z^n, d)$. Note that the codewords in each of $M_{og}^{(i)}(z^n, d), (M_s(z^n, d) \setminus M_{og}^{(i)}(z^n, d))$, and $M_s^c(z^n, d)$ are uniformly distributed in the respective spaces. We have two key steps using Lemma IV.4.

1. For every realization of $X^n(M_{og}^{(i)}(z^n, d))$, by considering $V = \cup_{w \in M_{og}^{(i)}(z^n, d)} \mathcal{B}(X^n(w) + s^n, (p + \epsilon_1)n)$ in Lemma IV.4, with probability at least $1 - e^{-\beta n^2}$, there are at most cn^2 messages in $M_s^c(z^n, d)$ with codewords X^n satisfying (4) for some $w \in M_{og}^{(i)}(z^n, d)$. So the same statement is also true over the random choice of $X^n(M_{og}^{(i)}(z^n, d))$.

2. Now, by Corollary IV.5, with probability at least $1 - e^{-\beta n^2}$, for every x^n , there are at most cn^2 codewords $X^n(M_{og}^{(i)}(z^n, d)) \cap \mathcal{B}(x^n + s^n, (p + \epsilon_1)n)$. This ensures that there are at most cn^2 codewords from $X^n(M_{og}^{(i)}(z^n, d))$ for which $x^n \in \mathcal{B}(X^n(w) + s^n, (p + \epsilon_1)n)$.

So, for every z^n, r , and s^n , with high probability over the code, there are at most $c^2 n^4$ codewords from $X^n(M_{og}^{(i)}(z^n, d))$ which satisfy the condition in the lemma. Finally, taking the union bound over all $i < \lambda(z^n, d)$, we have the result for $M_s^c(z^n, d)$.

The same proof steps also work for $M_s(z^n, d) \setminus M_{og}^{(i)}(z^n, d)$. We take $V = \left(\bigcup_{w \in M_{og}^{(i)}(z^n, d)} \mathcal{B}(X^n(w) + s^n, (p + \epsilon_1)n) \right) \cap Sh(z^n, d)$ in the first step. We note that $|V| \leq 2^{n(H(p+\epsilon_1)+\epsilon_2/2+\delta)}$ (for large enough n), $|Sh(z^n, d)| \geq 2^{n(H(q-\epsilon_1)-\epsilon_2/2)}$, and the number of messages in $M_s(z^n, d) \setminus M_{og}^{(i)}(z^n, d)$ is at most $2^{n(H(q+\epsilon_1)+R-1+\epsilon_2)}$. So, the expected number of these codewords in V is at most $2^{n(H(p+\epsilon_1)+H(q+\epsilon_1)-H(q-\epsilon_1)+R-1+2\epsilon_2+\delta)}$. The exponent is < 0 for small enough $\epsilon_2, \epsilon_1, \delta$. Thus the first step follows using the same arguments. The second step is the same as before. ■

In the following, we consider the codewords in $M_{og}^{(k)}(z^n, d)$ arranged in a square and indexed by a set $A \times A$ with $|A| = 2^{n\delta/2}$, before being randomly associated to the messages. With abuse of notation, for $i, j \in A$, we will denote the (i, j) -th codeword in this arrangement as $X^n(i, j)$ (note that this omits the global association of the codewords to the actual messages; to avoid this, we may further index these with (z^n, d, k)).

Lemma IV.7. *There exists $\beta > 0$ such that, for every z^n, d satisfying $|d - nq| \leq n\epsilon_1$, error s^n introduced by James, for every subset M of messages with $2^{n(H(d/n)+R-1+\epsilon_2)} \geq |M| \geq 2^{n(H(d/n)+R-1-\epsilon_2)}$, conditioned on $M_s(z^n, d) = M$, with probability at least $1 - e^{-\beta n^2}$ over the code, for every $k < \lambda(z^n, d)$, (i) for every i , there are at most $c^2 n^4$ codewords in the i -th row $\{X^n(i, j) | j \in A\}$ for which $\{X^n(i', j') | i' \neq i, j' \in A\} \cap \mathcal{B}(X^n(i, j) + s^n, (p + \epsilon_1)n)$ is non-empty, (ii) there are at most $2^{n(3\delta/4)}$ messages $w \in M_{og}^{(k)}(z^n, d)$ for which $\{X^n(w') | w' \in M_{og}^{(k)}(z^n, d), w' \neq w\} \cap \mathcal{B}(X^n(w) + s^n, (p + \epsilon_1)n)$ is non-empty.*

Proof: We fix a k and prove both parts; a union bound over all k at the end proves the lemma. *Part (i):* Recall that the codewords in $X^n(M_{og}^{(k)}(z^n, d))$ are drawn independently and uniformly from $Sh(z^n, d)$. The proof of this part then follows using a two-step argument similar to the proof of Lemma IV.6.

Part (i) implies that with high probability, there are at most $c^2 n^4$ codewords in each row of $M_{og}^{(k)}(z^n, d)$ which will be confused, under the error vector s^n , with some codeword in another row. The same statement also holds for columns by the same arguments.

Part (ii): By part (i), with high probability over the code, there are at most $c^2 n^4$ codewords in any row (and column) which are confusable, under the error vector s^n , with a codeword in another row. Let us now define a directed graph with vertices A^2 , and there is an edge from $X^n(i, j)$ to $X^n(i', j')$ if $d_H(X^n(i, j) + s^n, X^n(i', j')) \leq n(p + \epsilon_1)$, that is, if the codeword $X^n(i, j)$ is confusable under the error vector s^n with $X^n(i', j')$. We define the non-horizontal out-degree of a node as the number of edges coming out of that node to another node in a different row. The non-vertical out-degree is similarly defined. Clearly the out-degree of a node is at most the sum of the non-horizontal and non-vertical out-degree. Under the high probability event of part (i), each row of vertices in the graph has at most $c^2 n^4$ vertices with non-zero non-horizontal out-degree. So in the graph, there are at most $c^2 n^4 |A|$ nodes with non-zero non-horizontal out-degree. Similarly there are at most $c^2 n^4 |A|$ nodes with non-zero non-vertical out-degree. So there are at most $2c^2 n^4 |A| \leq 2^{n(3\delta/4)}$ nodes with non-zero out-degree. ■

Lemma IV.6 and IV.7 prove (3) for some $\beta > 0$, for all z^n, d, s, M satisfying $|d - nq| \leq \epsilon_1 n$ and $2^{n(H(d/n)+R-1+\epsilon_2)} \geq |M| \geq 2^{n(H(d/n)+R-1-\epsilon_2)}$. This in turn proves (1). Thus with high probability, the code satisfies $\mathcal{E}_{C1}, \mathcal{E}_{C2}$. Such a code then achieves exponentially small probability of error by (2). This completes the achievability proof of Theorem III.1.

V. GENERAL MYOPIC CHANNEL AND THE PROOF OF THEOREM III.4

A. Intuition for general myopic jamming channels

For general pairs of channels (a stochastic channel $p_{Z|X}$ and the AVC $p_{Y|XS}$), many of the ideas used in the achievability proofs for the bit-flipping channel also go through to result in the Theorems III.4, III.5, III.6. We highlight the major differences here.

Model: To begin with, we borrow heavily from the problem formulation in [18] to model the relationship between the n -letter tuple (X^n, Z^n, S^n, Y^n) in terms of single-letter distributions $p_X p_{Z|X} p_{S|Z} p_{Y|XS}$. More precisely:

- In our achievability proofs we focus on codebooks generated i.i.d. according to the distribution p_X (subject to the constraint $p_X \in \mathcal{V}$).
- The channels $p_{Z|X}$ and $p_{Y|XS}$ are specified as part of the problem statement, in which they are assumed to be memoryless.
- While James is free to choose any n -letter state-vector (subject to the constraint that the type-class of S^n be in \mathcal{W}) as a function of his full n -letter observation Z^n , any such choice can be “reverse engineered” as a particular length- n instantiation of a conditional distribution $p_{S|Z}$, where the $p_{S|Z}$ corresponds to the conditional type-class of S^n given the observed vector Z^n .
- Further, as defined in the myopic jamming problem statement, James’s state vector S^n must be conditionally independent of X^n given his observation Z^n .

Putting these together, we note that the n -letter tuple (X^n, Z^n, S^n, Y^n) can be thought of as a tuple of length- n sequences generated according to the single-letter distribution $p_X p_{Z|X} p_{S|Z} p_{Y|XS}$ (subject, of course, to the corresponding input and state constraints \mathcal{V} and \mathcal{W}).

Results: It is then natural to conjecture that the corresponding “capacity” of the problem equals $I(X; Y)$, maximized over all valid encoder profiles corresponding to p_X , and minimized over all valid attacks by James corresponding to $p_{S|Z}$, as long

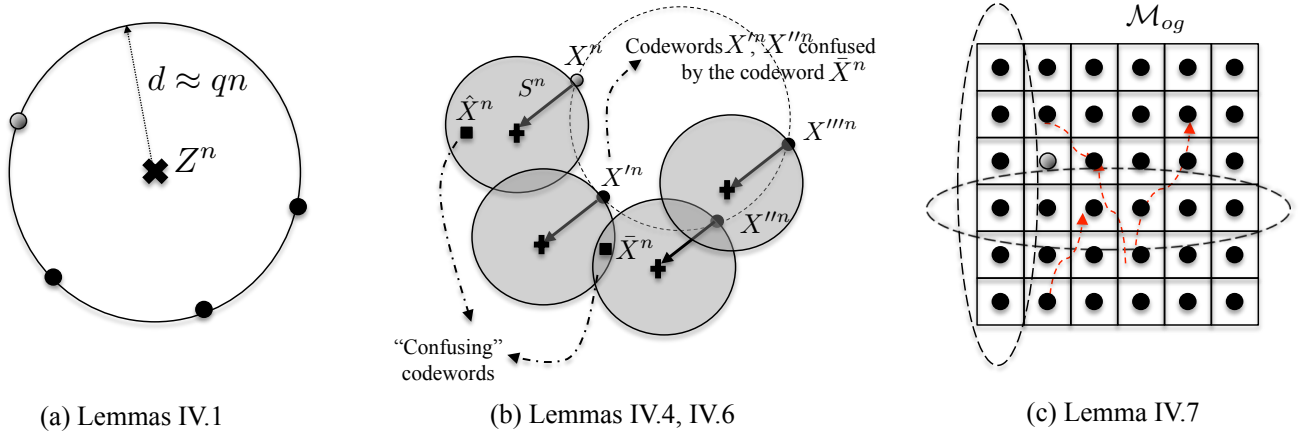


Fig. 6. Intuition about proof techniques: *Fig (a):* Lemma IV.1 uses “standard” concentration inequalities to argue that the value of d (the amount of noise James sees) is “close” to qn . Lemma IV.2 argues that for *every* shell with such d , the number of codewords on a shell of radius d centred at Z^n is close to $2^{n(H(q)-H(p))}$ – from James’s perspective, each of these codewords is equally likely to have been transmitted. *Fig (b):* Lemmas IV.4 and IV.6 are “list-decoding” lemmas. Lemma IV.4 argues that regardless of the shape of the volume being considered, as long as it is smaller than the “average volume per codeword”, for a super-exponentially large fraction of codes the number of codewords in the volume is not large (at most $\mathcal{O}(n^2)$). Lemma IV.6 then uses this result to show that there are not too many codewords in \mathcal{M}_{og} “confused by S^n with codewords in $\mathcal{C} \setminus \mathcal{M}_{og}$ ” (at most $\mathcal{O}(n^4)$). It does this in two steps – it first uses Lemma IV.4 to show that there are not too many “confuse-ing” codewords from $\mathcal{C} \setminus \mathcal{M}_{og}$ (e.g. \hat{X}^n and \tilde{X}^n in the figure), and then it re-uses Lemma IV.4 to show that each “confuse-ing” codeword does not lead to too many “confus-ed” codewords (\bar{X}^n only confuses X'^n and X''^n in the figure). *Fig (c):* Lemma IV.7 analogously proves that there are not too many codewords in \mathcal{M}_{og} “confused by S^n with other codewords in \mathcal{M}_{og} ”. To do so, the $2^{n\delta}$ codewords in \mathcal{M}_{og} are arranged in a square grid. Using Lemma IV.4 one can show that in any column (respectively row) of this grid there are not too many (at most $\mathcal{O}(n^2)$) codewords in that column (respectively row) that are confused by S^n with any other codeword in any other column (respectively row) – the red-arrows in the figure indicate codewords that are confused by S^n with another codeword in a different row or column. This allows one to demonstrate that the total fraction of codewords in \mathcal{M}_{og} that are confused by S^n is an exponentially small fraction, and hence the probability of error is small. Since the preceding statements are true with probability super-exponentially close to 1, one may take a union bound over all possible values of d , Z^n , and S^n .

as the channel $p_{Z|X}$ is “sufficiently myopic” compared to the channel $p_{Y|XS}$. And indeed both our achievability and converse expressions (in Theorems III.4, III.5) take this form. However, there is a gap between the tightest converse we can prove in Theorem III.5, and the achievability we can prove in Theorem III.4. Specifically, our achievability requires us to maximize over p_X such that two “myopicity” conditions (given by (b) and (c) in the statement of Theorem III.4) are satisfied.

For a wide variety of other myopic channel-pairs our approach results in non-trivial achievability results. This includes problems in which the channels from Alice to James, and from Alice to Bob, are of different “forms” (for instance, a BSC(q) from Alice to James, and an AVC from Alice to Bob in which James can *erase* a fraction p of bits). However, we are by no means convinced that the achievability result we present is optimal in general. In particular, while the first myopicity condition (Theorem III.4 (b)), $I(X; Z) < I(X; Y)$ is “somewhat natural” (corresponding to James having a weaker channel than any channel he can impose on Bob), the second condition (Theorem III.4 (c)) arises from somewhat technical considerations in “reverse list-decoding” described below.

Proof Techniques: Given the problem formulation described above, many (but not all) of the ideas described in the achievability proof of the channel $C(q, p)$ carry through. Specifically:

- The oracle-given set is defined in an analogous manner to how it is defined for the channel $C(q, p)$. Specifically, as long as $I(X; Z) < I(X; Y)$, one can demonstrate via standard combinatorial arguments that all “typical type-classes” have exponentially many codewords in them – one then constructs the corresponding oracle-given set by choosing sufficiently many codewords with the same empirical conditional distribution $p_{X|Z}$ as the “true” (X^n, Z^n) .
- One can then show that over the randomness in which codeword X^n in the oracle-given set was actually transmitted, with high probability the tuples (X^n, S^n, Y^n) are jointly typical according to the joint distribution $p_X p_{Z|X} p_{S|X} p_{Y|XS}$.
- For state-deterministic channels⁵ $p_{Y|XS}$ one can show an “ X^n ”-list-decoding argument. Namely, one can show that with probability super-exponentially close to one over code design, the number of codewords from the oracle-given set that are translated under the action of a feasible state vector S^n into the conditionally typical set w.r.t. any typical Y^n is “small” (at most $\mathcal{O}(n^2)$).
- We also use a “ Y^n ”-list-decoding argument, that demonstrates that the number of Y^n resulting from the action by a fixed feasible state vector S^n acting on any X^n from the oracle-given set is at most $\mathcal{O}(n^2)$. Again, for technical reasons, to prove this list-decoding result we need to impose some additional constraints on the class of permissible states \mathcal{W} – these are precisely the constraints in Theorem III.4(c).

⁵The restriction to state-deterministic channels is a technical condition required by our proof, so as to be able to achieve the claimed rate. Removing this restriction is possible, but then with our current proof techniques our achievable rates reduce to $I(X; Y) - H(Y|X, S)$ rather than $I(X; Y)$, and also we need to further restrict the class of state constraints \mathcal{W} for which such a result is possible. Attempting to remove this restriction is a direction of ongoing research. Nonetheless, the class of state-deterministic channels already contains many interesting myopic channels problems, such as the channel $C(q, p)$ discussed in length above, the channel $CE(q, p)$ discussed in Sec. III-C, and a variety of other “mixed” channels.

- Finally, the square-grid argument described in the proof of the $C(q, p)$ is essentially unchanged in this general setting.
- As in the $C(q, p)$ case, the interplay between the problems of jamming-resilient and eavesdropping-resilient code-designs is natural. As in the general wiretap-channel case, one can indeed use our codes, as outlined in Theorem III.4, and transmit over them messages that themselves comprises of the “true message”, padded with random bits, and encoded via wiretap-channel codes, so as to guarantee communication that is both reliable against James’s jamming, and secure against his eavesdropping.

B. Proof of Theorems III.4

Let $T(x^n, z^n)$ denote the joint type of the vectors x^n, z^n . Our achievability scheme is using a random code. Let p_X be the input distribution used to construct the code. We assume that it satisfies the condition in Theorem III.4. Recall that $p_{Z|X}$ is Calvin’s channel law. These give a joint distribution p_{XZ} and a marginal distribution p_Z . The channel law to Bob is given by $p_{Y|XS}$. Note that every i.i.d. jamming strategy $p_{S|Z}$ results in a joint distribution $p_X p_{Z|X} p_{S|Z} p_{Y|XS}$. We define

$$\mathcal{W}_{S|Z} := \{p_{S|Z} \mid (p_X p_{Z|X} p_{S|Z})_S \in \mathcal{W}\},$$

where $(p_X p_{Z|X} p_{S|Z})_S$ denotes the marginal of $p_X p_{Z|X} p_{S|Z}$ on S . In the following, we assume the distributions $p_X, p_{Z|X}, p_{Y|XS}$ to be fixed.

For any y^n , let us define $\mathcal{B}_{X|Y}(y^n, \mathcal{W})$ as the set of x^n which are jointly ϵ_1 -typical with y^n for some $p_{S|Z} \in \mathcal{W}_{S|Z}$. The volume of $\mathcal{B}_{X|Y}(y^n, \mathcal{W})$ can be bounded as

$$\frac{1}{n} \log_2 |\mathcal{B}_{X|Y}(y^n, \mathcal{W})| \leq \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y) + f_1(\epsilon_1)$$

for some $f_1(\epsilon_1) \rightarrow 0$ as $\epsilon_1 \rightarrow 0$. Similarly, $\mathcal{B}_{Y|X}(x^n, \mathcal{W})$ is defined, and it has a volume $\leq \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) + f_1(\epsilon_1)$. Drawing similarity with the proofs for $C(q, p)$, these sets take the role of balls of radius p around x^n and y^n respectively.

Decoding: On receiving y^n , if Bob finds a unique codeword in $\mathcal{B}_{X|Y}(y^n, \mathcal{W})$, then he decodes this codeword. Otherwise he declares error.

The overall proof argument is the same as in the bit-flip case. So we only give the relevant modified lemmas and definitions in the following, in addition to any extra arguments which are required for the general case.

Let τ denote a joint type of x^n, z^n . In the following, for a given z^n , τ denotes a joint type that is consistent with z^n .

$$\mathcal{S}h(z^n, \tau) := \{x^n \in \mathcal{X}^n : T(x^n, z^n) = \tau\}.$$

Let T denote the type of $(X^n(W), Z^n)$. We also denote by $\mathcal{T}_\mu(X, Z)$, the set of joint types which are μ -typical. Here $\mu = \mu(\epsilon_1)$ (it is a function of $p_X, p_{Z|X}$, though we do not mention it explicitly).

We define events, similar to those in the proof for the $C(q, p)$,

$$\begin{aligned} \mathcal{E}_{C1}(z^n, \tau) &:= \left\{ 2^{n(H_\tau(X|Z) + R - H(X) + \epsilon_2)} \geq |\{w : X^n(w) \in \mathcal{S}h(z^n, \tau)\}| \geq 2^{n(H_\tau(X|Z) + R - H(X) - \epsilon_2)} \right\} \\ \mathcal{E}_{C1} &:= \cap_{z^n, \tau \in \mathcal{T}_\mu(X, Z)} \mathcal{E}_{C1}(z^n, \tau) \\ \mathcal{E}_D &:= \{T \in \mathcal{T}_\mu(X, Z)\}. \end{aligned}$$

Here $H_\tau(X|Z)$ denotes the conditional entropy for the joint distribution τ . For every z^n , and $\tau \in \mathcal{T}_\mu(X, Z)$, the oracle partitions the set of messages

$$M_s(z^n, \tau) = \{w : X^n(w) \in \mathcal{S}h(z^n, \tau)\}$$

with codewords on the shell $\mathcal{S}h(z^n, \tau)$ into disjoint subsets $M_{og}^{(1)}(z^n, \tau), M_{og}^{(2)}(z^n, \tau), \dots, M_{og}^{(\lambda(z^n, \tau))}(z^n, \tau)$ of size $2^{n\delta}$, except possibly the last subset with smaller size. The oracle reveals T and the particular subset $\mathcal{M}_{og} = M_{og}^{(i)}(Z^n, T)$ of $M_s(Z^n, T)$ that contains the encoded message W .

In the general case under consideration, τ, T respectively take the role of d and D in the binary case. Like in the binary case, Lemmas IV.1 and IV.2 also hold here with the changed definitions of \mathcal{E}_D and \mathcal{E}_{C1} . h_2 now depends on $p_{Z|X}, \mathcal{W}, \epsilon, \epsilon_1, \epsilon_2$. With D replaced by T , and the changed definition of $\mathcal{S}h(Z^n, D) := \mathcal{S}h(Z^n, T)$, the observations O.1, O.2, O.3, and Lemma IV.3 in the previous section still hold.

Suppose $\tau \in \mathcal{T}_\mu(X, Z)$. The event $\mathcal{E}_{C2}(z^n, \tau, s^n)$ is defined, similarly as before, over the code construction that every subset of size $2^{n\delta}$ in the ordered partition of $M_s(z^n, \tau)$ has at most only $2^{n(3\delta/4)}$ messages which will undergo decoding error for the respective realizations of D, Z^n, S^n, W . The event \mathcal{E}_{C2} is defined, also similarly as before, as

$$\mathcal{E}_{C2} = \cap_{z^n, \tau, s^n} \mathcal{E}_{C2}(z^n, \tau, s^n)$$

where the intersection is over $\tau \in \mathcal{T}_\mu(X, Z)$, all feasible s^n , and all z^n .

We need to show the counterpart of (3):

$$\Pr(\mathcal{E}_{C2}^c(z^n, \tau, s^n) | M_s(z^n, \tau) = M) \leq e^{-\beta n^2}. \quad (5)$$

for every M satisfying $2^{n(H_\tau(X|Z)+R-H(X)+\epsilon_2)} \geq |M| \geq 2^{n(H_\tau(X|Z)+R-H(X)-\epsilon_2)}$. The overall proof argument is the same as in the binary case. We first note the fact that for large enough n , for any $X^n \in \mathcal{Sh}(z^n, \tau)$ and s^n satisfying \mathcal{W} , $X^n \in \mathcal{B}_{X|Y}(s^n(X^n), \mathcal{W})$. So the transmitted codeword always satisfies the decoding condition. This is because, (i) $X - Z - S$ forms a Markov chain, (ii) (X^n, z^n) is $\epsilon_1/2$ -typical, (iii) (z^n, s^n) is $\epsilon_1/2$ -typical for some $p_{S|Z} \in \mathcal{W}_{S|Z}$. To see why the third statement is true, we note that z^n is μ -typical, and s^n satisfies \mathcal{W} . The conditional distribution $p_{S|Z} := T(z^n)T(s^n|z^n)/p_Z$ (at all points with $p_Z(z) \neq 0$) is in $\mathcal{W}_{S|Z}$, and (z^n, s^n) is $\epsilon_1/2$ -typical for this $p_{S|Z}$ if μ is small enough.

We now give the counterparts of Lemma IV.6 and Lemma IV.7 below. Together, they imply (5). But first we give a generalization of Lemma IV.4:

Lemma V.1. *Let $V \subset \mathcal{X}^n$ be a subset of ϵ_1 -typical sequences w.r.t. the distribution p_X with cardinality $|V| \leq 2^{nc}$. Then (i) the probability $\Pr_{p_X}(V) \leq 2^{-n(H(X)-c-f_2(\epsilon_1))}$ for some $f_2(\epsilon_1) \rightarrow 0$ as $\epsilon_1 \rightarrow 0$, (ii) if $R < H(X) - c - f_2(\epsilon_1)$, and 2^{nR} vectors $X^n(w); w = 1, 2, \dots, 2^{nR}$ are chosen independently with i.i.d. $\sim p_X$ components, then for a sufficiently large constant α , $\Pr(|\{w : X^n(w) \in V\}| > cn^2) \leq e^{-\alpha n^2/6}$.*

Proof: Part (i) follows as the probability of each ϵ_1 -typical sequence is $\leq 2^{-n(H(X)-f_2(\epsilon_1))}$. Part (ii) follows using part (i) in a similar way as Lemma IV.4 using the Chernoff bound. ■

Lemma V.2. *There exists $\beta > 0$ such that for every $z^n, \tau \in \mathcal{T}_\mu(X, Z)$, state vector s^n introduced by Calvin, for every subset M of messages with $2^{n(H_\tau(X|Z)+R-H(X)+\epsilon_2)} \geq |M| \geq 2^{n(H_\tau(X|Z)+R-H(X)-\epsilon_2)}$, conditioned on $M_s(z^n, \tau) = M$, with probability at least $1 - e^{-\beta n^2}$ over the code, for every $i < \lambda(z^n, \tau)$, there are at most $c^2 n^4$ codewords from $X^n(M_{og}^{(i)}(z^n, \tau))$ for which there is a codeword from $X^n((M_{og}^{(i)}(z^n, \tau))^c)$ which lies in $\mathcal{B}_{X|Y}(s^n(X^n(w)), \mathcal{W})$.*

Proof: Clearly, $(M_{og}^{(i)}(z^n, \tau))^c = M_s^c(z^n, \tau) \cup (M_s(z^n, \tau) \setminus M_{og}^{(i)}(z^n, \tau))$. Note that the codewords in $(M_s(z^n, \tau) \setminus M_{og}^{(i)}(z^n, \tau))$ are uniformly distributed in $\mathcal{Sh}(z^n, \tau)$. The codewords of $M_s^c(z^n, \tau)$ are chosen according to p_X^n conditioned on the subset $(\mathcal{Sh}(z^n, \tau))^c$. We first prove the statement for codewords in $M_s^c(z^n, \tau)$. We have two key steps:

1. For every realization of $X^n(M_{og}^{(i)}(z^n, \tau))$, we consider $V = \bigcup_{w \in M_{og}^{(i)}(z^n, \tau)} \mathcal{B}_{X|Y}(s^n(X^n(w)), \mathcal{W})$. This satisfies $(1/n) \log_2 |V| \leq \delta + f_1(\epsilon_1) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y)$. Since $\mathcal{Sh}(z^n, \tau)$ contains only a subset of one type of x^n , for large enough n , under the probability measure p_X^n , $\Pr(\mathcal{Sh}(z^n, \tau)) \leq 1/2$. Thus by Lemma V.1(i), for the codeword of any message $w \in M_s^c(z^n, \tau)$, the probability of it being chosen from V is

$$\begin{aligned} & \Pr(V | (\mathcal{Sh}(z^n, \tau))^c) \\ & \leq 2 \cdot 2^{-n(H(X)-\delta-f_1(\epsilon_1)-f_2(\epsilon_1)-\max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y))} \\ & = 2 \cdot 2^{-n(\min_{p_{S|Z} \in \mathcal{W}_{S|Z}} I(X;Y)-\delta-f_1(\epsilon_1)-f_2(\epsilon_1))} \end{aligned}$$

Thus, by the same proof as that of Lemma V.1 (ii), with probability at least $1 - e^{-\beta n^2}$, there are at most cn^2 codewords from $X^n(M_s^c(z^n, \tau))$ in V for sufficiently small δ, ϵ_1 . Here we have used the fact that $R < \min_{p_{S|Z} \in \mathcal{W}_{S|Z}} I(X;Y) - \delta - f_1(\epsilon_1) - f_2(\epsilon_1)$. So the same statement is also true over the whole random code, that is, when $X^n(M_{og}^{(i)}(z^n, \tau))$ is also chosen randomly.

2. Now, over the random choice of $X^n(M_{og}^{(i)}(z^n, \tau))$ from the vectors in $\mathcal{Sh}(z^n, \tau)$, with probability at least $1 - e^{-\beta n^2}$, for every x^n , there are at most cn^2 codewords from $X^n(M_{og}^{(i)}(z^n, \tau))$ in $(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))$. Here $(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W})) := \{x^{n'} : s^n(x^{n'}) \in \mathcal{B}_{Y|X}(x^n, \mathcal{W})\}$. This follows using Lemma V.1 because, for every feasible s^n , $(1/n) \log_2 |(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))| \leq \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y, S) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) < H(X|Z)$.

Now the proof follows by taking the union bound over all $i < \lambda(z^n, \tau)$ as in the binary case (Lemma IV.6). A similar proof also works for $M_s(z^n, \tau) \setminus M_{og}^{(i)}(z^n, \tau)$ by noting that the volume of the shell is $\geq 2^{n(H_\tau(X|Z)-\epsilon_2/2)}$ (for large enough n), and the number of codewords on the shell is $|M| \leq 2^{n(H_\tau(X|Z)+R-H(X)+\epsilon_2)}$. ■

Similar to the binary case, let us consider the codewords in $M_{og}^{(k)}(z^n, \tau)$ arranged in a square and indexed by a set $A \times A$ with $|A| = 2^{nh_2(\epsilon_1, \epsilon_2)/2}$.

Lemma V.3. *There exists $\beta > 0$ such that, for every $z^n, \tau \in \mathcal{T}_\mu(X, Z)$, state s^n introduced by Calvin, for every subset M of messages with $2^{n(H_\tau(X|Z)+R-H(X)+\epsilon_2)} \geq |M| \geq 2^{n(H_\tau(X|Z)+R-H(X)-\epsilon_2)}$, conditioned on $M_s(z^n, \tau) = M$, with probability at least $1 - e^{-\beta n^2}$ over the code, for every $k < \lambda(z^n, \tau)$, (i) for every i , there are at most $c^2 n^4$ codewords in the i -th row $\{X^n(i, j) | j \in A\}$ for which $\{X^n(i', j') | i' \neq i, j' \in A\} \cap \mathcal{B}_{X|Y}(s^n(X^n(i, j)), \mathcal{W})$ is non-empty, (ii) there are at most $2^{n(3\delta/4)}$ messages $w \in M_{og}^{(k)}(z^n, \tau)$ for which $\{X^n(w') | w' \in M_{og}^{(k)}(z^n, \tau), w' \neq w\} \cap \mathcal{B}_{X|Y}(s^n(X^n(w)), \mathcal{W})$ is non-empty.*

Proof: The proof of the first part follows using a two-step argument similar to the proof of Lemma V.2. The proof of the second part follows using similar arguments as the second part of Lemma IV.7. ■

Lemma V.2 and V.3 prove (5), and then by the same arguments as in the bit-flip case, the achievability of Theorem III.4 follows.

Remark V.4 (Improvements for bit erasing and flipping adversaries). *Condition (c) on an achievable rate in Theorem III.4 is due to the bound*

$$(1/n) \log_2 |(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))| \leq \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(X|Y, S) + \max_{p_{S|Z} \in \mathcal{W}_{S|Z}} H(Y|X) \quad (6)$$

used in the second part of the proof of Lemma V.2. In general, (6) is the best bound we have in single-letter expression for $(1/n) \log_2 |(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))|$. We suspect this to be quite loose, and expect the result (Theorem III.4) for general channels to hold under weaker conditions than (c).

(i) *Binary erasure-erasure channel:* For the erasure-erasure channel $CE(q, p)$, this condition gives $p + H(p) < q$, which is stronger than the natural ‘sufficiently myopic’ condition $p < q$. For this channel, it is possible to get a tighter bound which results in the condition $p < q$, that is the same as condition (b). We first note that $|(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))|$ counts the number of vectors $x^{n'}$ for which $s^n(x^{n'})$ can also be obtained by erasing some components of x^n . The components of x^n erased in this process must be the same as those indicated by s^n , that is, $s^{n'}(x^n) = s^n(x^{n'})$ only if $s^n = s^{n'}$. Thus,

$$(1/n) \log_2 |(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))| \leq p,$$

as the number of erasures in s^n is at most np . Thus under condition (b) alone, i.e., $p < q$, the capacity of $CE(q, p)$ is $1 - p$. This proves Theorem III.8.

(ii) *Bit erasing and flipping adversary, $CEF(p_{Z|X}, p_e, p_w)$:* We note that the counting of $|(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))|$ only involves the channel between Alice to Bob (the AVC), and not the channel between Alice to James. So similar improved counting as for the erasure-erasure channel works as long as James can only erase and flip transmitted bits. For such adversaries, irrespective of James’s own channel, Theorem III.4 holds without the extra condition (c).

In particular, let us consider the setup $CEF(p_{Z|X}, p_e, p_w)$ where James can erase upto p_e fraction of the transmitted bits, and he can flip upto p_w fraction of the transmitted bits. For such a valid state vector s^n , let s_e^n denote the action of erasing the same positions that are erased by s^n . Now clearly,

$$(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W})) = \{x^{n'} | d_H(s^n(x^{n'}), s_e^n(x^n)) \leq p_w n\}.$$

Thus

$$(1/n) \log_2 |(s^n)^{-1}(\mathcal{B}_{Y|X}(x^n, \mathcal{W}))| \leq p_e + (1 - p_e) H\left(\frac{p_w}{1 - p_e}\right).$$

This gives an achievable rate upto

$$\begin{aligned} & 1 - \left(p_e + (1 - p_e) H\left(\frac{p_w}{1 - p_e}\right) \right) \\ &= (1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right) \right) \end{aligned}$$

under the sufficient myopicity condition that

$$1 - H(X|Z) \leq (1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right) \right)$$

(iii) *Secrecy capacity for the erasing and flipping adversary, $CEF(p_{Z|X}, p_e, p_w)$:* Using a standard stochastic encoding technique for wiretap channels, the above also gives a secrecy rate of

$$\begin{aligned} & (1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right) \right) - (1 - H(X|Z)) \\ &= H(X|Z) + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right). \end{aligned}$$

For the special case of $CEF(BEC(q), p_e, p_w)$, this gives the secrecy rate

$$\begin{aligned} & (1 - p_e) \left(1 - H\left(\frac{p_w}{1 - p_e}\right) \right) - (1 - q) \\ &= q + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right). \end{aligned}$$

(iv) *Secrecy against a type II wiretapper adversary:* We now elaborate on the erasure-erasure setting and explicitly on extending Theorem III.10 to the model of Aggarwal et al. [22]. In general, the proof of Theorem III.10 follows that of Theorem III.6 when one considers the channel $CE(q, p)$. Specifically, the proof of secrecy for rates under $q - p$ follows roughly by appending $1 - q$ bits of private randomness r to the message u , and applying our code on the concatenated pair (u, r) (which is of length $(1 - p)n$). To prove that our random code construction satisfies the secrecy requirement $\frac{1}{n}I(Z^n; U) < \varepsilon$ in the model of [22] (when James can pick which qn bits are erased) one must show that with high probability over code design, for every view Z^n of James, for every $u \in U$ there are approximately the same number of random strings r such that the encoding of (u, r) is consistent with Z^n (i.e., the corresponding codeword agrees with Z^n on all the un-erased entries). Indeed, in this case, the amount of information James has on U is limited. Let $\varepsilon > 0$. Taking the size of r to be $1 - q + \varepsilon$ and the rate of u to be $q - p - 2\varepsilon$, we have (via the Chernoff bound) with doubly exponential probability of $1 - 2^{-2^{\Omega(\varepsilon n)}}$ over code design that for every view Z^n of James and every $u \in U$ the number of different random r such that the encoding of (u, r) is consistent with Z^n is in the range $[2^{\varepsilon n}(1 - \varepsilon), 2^{\varepsilon n}(1 + \varepsilon)]$. Bounding entropy by variational distance we conclude that $\frac{1}{n}I(Z^n; U) < O(\varepsilon)$.

(v) *Wiretap channel of type II with erasing and flipping adversary, $WCEF-II(p_r, p_e, p_w)$:* If James can choose a $p_r = 1 - q$ fraction of transmitted bits to observe, then using the lines of argument outlined above, it can be seen that the secrecy rate $q + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right) = 1 - p_r + p_e H\left(\frac{p_w}{1 - p_e}\right) - p_e - H\left(\frac{p_w}{1 - p_e}\right)$ is still achievable.

VI. CONCLUSIONS

In this work we study the secure and standard capacity of adversarial myopic channels. For the bit-flipping adversarial channel $C(q, p)$, for the binary erasure-erasure adversarial channel $CE(q, p)$, and more generally for binary input channels where the adversary can both erase and flip some fractions of bits, we characterize these capacities as the capacity under random noise when the adversary's own channel is more noisy than the worst noise it can impose on Bob, in terms of mutual information. For these models, we also consider analogs of the wiretap channel of type II. For general myopic channels, we prove similar achievability results under a stricter condition of myopicity. A tight characterization of capacity for general myopic channels is left open and subject of future work.

VII. ACKNOWLEDGEMENT

The work of B. K. Dey was supported in part by Bharti Centre for Communication, IIT Bombay, a grant from the Department of Science and Technology, Government of India, and a grant from ITRA, Government of India. S. Jaggi's work was partially supported by a grant from University Grants Committee of the Hong Kong, Special Administrative Region, China (Project No. AoE/E-02/08), and by the Innovation Technology Fund (ITF) Project ITS/143/14FP, Innovation Technology Commission, the Government of HKSAR. The work of M. Langberg was supported in part by NSF grant no. 1321129.

REFERENCES

- [1] Bikash Kumar Dey, Sidharth Jaggi, and Michael Langberg. Sufficiently myopic adversaries are blind. In *IEEE International Symposium on Information Theory*, pages 1164–1168, 2015.
- [2] Claude E. Shannon and Warren Weaver. *The mathematical theory of communication*. University of Illinois Press IL, 1949.
- [3] Michael Langberg. Oblivious channels and their capacity. *IEEE Transactions on Information Theory*, 54(1):424–429, 2008.
- [4] Richard W Hamming. Error detecting and error correcting codes. *Bell System technical journal*, 29(2):147–160, 1950.
- [5] David Blackwell, Leo Breiman, and A. J. Thomasian. The capacities of certain channel classes under random coding. *The Annals of Mathematical Statistics*, pages 558–567, 1960.
- [6] Rudolf Ahlswede. Elimination of correlation in random codes for arbitrarily varying channels. *Probability Theory and Related Fields*, 44(2):159–175, 1978.
- [7] Imre Csiszar and Prakash Narayan. The capacity of the arbitrarily varying channel revisited: Positivity, constraints. *IEEE Transactions on Information Theory*, 34(2):181–193, 1988.
- [8] Imre Csiszar and Prakash Narayan. Capacity of the gaussian arbitrarily varying channel. *IEEE Transactions on Information Theory*, 37(1):18–26, 1991.
- [9] Bikash Kumar Dey, Sidharth Jaggi, and Michael Langberg. Codes against online adversaries. In *47th Annual Allerton Conference on Communication, Control, and Computing*, pages 1169–1176, 2009.
- [10] Michael Langberg, Sidharth Jaggi, and Bikash Kumar Dey. Binary causal-adversary channels. In *IEEE International Symposium on Information Theory*, pages 2723–2727, 2009.
- [11] Bikash Kumar Dey, Sidharth Jaggi, Michael Langberg, and Anand D. Sarwate. Coding against delayed adversaries. In *IEEE International Symposium on Information Theory*, pages 285–289, 2010.
- [12] Ishay Haviv and Michael Langberg. Beating the gilbert-varshamov bound for online channels. In *IEEE International Symposium on Information Theory*, pages 1392–1396, 2011.
- [13] Bikash Kumar Dey, Sidharth Jaggi, Michael Langberg, and Anand D. Sarwate. Improved upper bounds on the capacity of binary channels with causal adversaries. In *IEEE International Symposium on Information Theory*, pages 681–685, 2012.
- [14] B. K. Dey, S. Jaggi, and M. Langberg. Codes against online adversaries, Part I: Large alphabets. *IEEE Transactions on Information Theory*, 59(6):3304–3316, 2013.
- [15] Bikash Kumar Dey, Sidharth Jaggi, Michael Langberg, and Anand D. Sarwate. Upper bounds on the capacity of binary channels with causal adversaries. *IEEE Transactions on Information Theory*, 59(6):3753–3763, 2013.
- [16] Zitan Chen, Sidharth Jaggi, and Michael Langberg. A characterization of the capacity of online (causal) binary channels. *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, pages 287–296, 2015.
- [17] Venkatesan Guruswami and Adam Smith. Codes for computationally simple channels: Explicit constructions with optimal rate. In *51st Annual IEEE Symposium on Foundations of Computer Science*, pages 723–732, 2010.

- [18] Anand D. Sarwate. Coding against myopic adversaries. In *IEEE Information Theory Workshop (ITW)*, pages 1–5, 2010.
- [19] Edgar N. Gilbert. A comparison of signalling alphabets. *Bell System Technical Journal*, 31(3):504–522, 1952.
- [20] R. R. Varshamov. Estimate of the number of signals in error correcting codes. In *Dokl. Akad. Nauk SSSR*, volume 117, pages 739–741, 1957.
- [21] Robert J. McEliece, Eugene R. Rodemich, Howard Rumsey Jr, and Lloyd R. Welch. New upper bounds on the rate of a code via the delarte-MacWilliams inequalities. *IEEE Transactions on Information Theory*, 23(2):157–166, 1977.
- [22] Vaneet Aggarwal, Lifeng Lai, A Robert Calderbank, and H Vincent Poor. Wiretap channel type II with an active eavesdropper. In *IEEE International Symposium on Information Theory*, pages 1944–1948. IEEE, 2009.
- [23] Carol Wang. On the capacity of the binary adversarial wiretap channel. *arXiv preprint arXiv:1605.01330v2*, 2016.
- [24] Ebrahim MolavianJazi, Matthieu Bloch, and J Nicholas Laneman. Arbitrary jamming can preclude secure communication. In *47th Annual Allerton Conference on Communication, Control, and Computing*, pages 1069–1075. IEEE, 2009.
- [25] I Bjelaković, Holger Boche, and Jochen Sommerfeld. Secrecy results for compound wiretap channels. *Problems of Information Transmission*, 49(1):73–98, 2013.
- [26] Janis Nötzel, Moritz Wiese, and Holger Boche. The arbitrarily varying wiretap channel – secret randomness, stability, and super-activation. *IEEE Transactions on Information Theory*, 62(6):3504–3531, 2016.
- [27] Moritz Wiese, Janis Nötzel, and Holger Boche. The arbitrarily varying wiretap channel—deterministic and correlated random coding capacities under the strong secrecy criterion. *arXiv preprint arXiv:1410.8078*, 2014.
- [28] Shabnam Shafiee and Sennur Ulukus. Mutual information games in multiuser channels with correlated jamming. *IEEE Transactions on Information Theory*, 55(10):4598–4607, 2009.
- [29] Anand D. Sarwate. An AVC perspective on correlated jamming. In *IEEE International Conference on Signal Processing and Communications (SPCOM)*, pages 1–5, 2012.
- [30] Pengwei Wang and Reihaneh Safavi-Naini. A model for adversarial wiretap channels. *IEEE Transactions on Information Theory*, 62(2):970–983, 2016.
- [31] Reihaneh Safavi-Naini and Pengwei Wang. A model for adversarial wiretap channels and its applications. *Journal of information processing*, 23(5):554–561, 2015.
- [32] Pengwei Wang and Reihaneh Safavi-Naini. An efficient code for adversarial wiretap channel. In *IEEE Information Theory Workshop (ITW)*, pages 40–44, 2014.
- [33] Reihaneh Safavi-Naini and Pengwei Wang. Codes for limited view adversarial channels. In *IEEE International Symposium on Information Theory*, pages 266–270, 2013.
- [34] Reihaneh Safavi-Naini and Pengwei Wang. Efficient codes for limited view adversarial channels. In *IEEE Conference on Communications and Network Security (CNS)*, pages 215–223, 2013.
- [35] Pengwei Wang, Reihaneh Safavi-Naini, and Fuchun Lin. Erasure adversarial wiretap channels. In *53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 1061–1068, 2015.
- [36] Pengwei Wang. *Secure Communication over Adversarial Channel*. PhD thesis, University of Calgary, 2015.
- [37] Qiaosheng Zhang, Swanand Kadhe, Mayank Bakshi, Sidharth Jaggi, and Alex Sprintson. Coding against a limited-view adversary: The effect of causality and feedback. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2530–2534, 2015.
- [38] Qiaosheng Zhang, Swanand Kadhe, Mayank Bakshi, Sidharth Jaggi, and Alex Sprintson. Talking reliably, secretly, and efficiently: A “complete” characterization. In *IEEE Information Theory Workshop (ITW)*, pages 1–5, 2015.
- [39] Swanand Kadhe, Alex Sprintson, Qiaosheng Eric Zhang, Mayank Bakshi, and Sidharth Jaggi. Reliable and secure communication over adversarial multipath networks: A survey. In *10th International Conference on Information, Communications and Signal Processing (ICICSP)*, pages 1–5, 2015.
- [40] Yingbin Liang, Gerhard Kramer, H Vincent Poor, and Shlomo Shamai. Compound wiretap channels. *EURASIP Journal on Wireless Communications and Networking*, 2009(1):1–12, 2009.
- [41] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.
- [42] Noga Alon and Joel H Spencer. *The probabilistic method*. John Wiley & Sons, 2004.